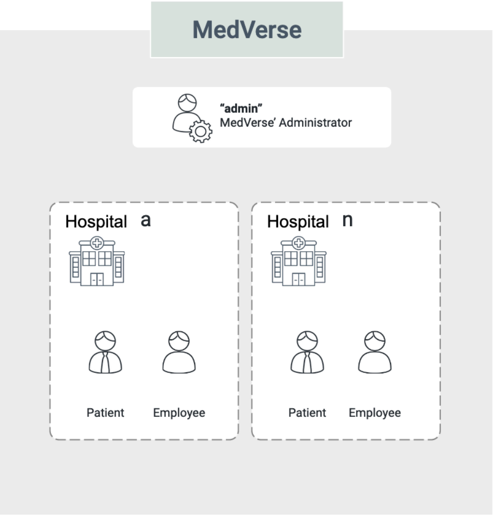
B2B CIAM

If you have a business that offers Business-to-Business (B2B) solutions, you need to define the structure of your organization in WSO2 Identity Server so as to represent all your partner/supplier organizations. You can then share your applications and services with your partner/supplier organizations and allow them to manage their own identity and access management requirements.

- All partner/supplier organizations of your business should be set up as organizations of your organization (root) in WSO2 Identity Server.
- Once the organizations are set up, you should onboard administrators to them. These Administrators can then use a separate administration portal created using WSO2 Identity Server's B2B APIs to manage their respective organizations.
- The organization (root) needs to share applications with its organizations so that the users managed by the organizations can log in and use them.

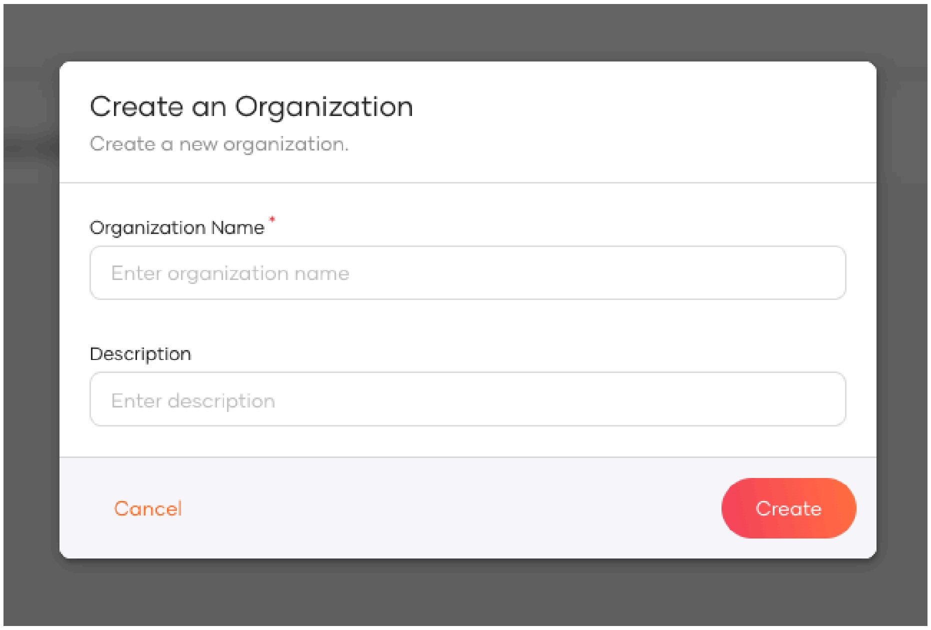


Let's use the use case in the diagram to demonstrate how we can configure Organization, Users and Applications to cater a B2B use case. As you can see, **admin** is the super Administrator of MedVerse. MedVerse has two Hospitals registered Hospital a and Hospital n. Each hospital has patients and employees registered separately.

Hospital a uses MFA for the authentication of patients whereas Hospital n uses only basic authentication. This can be configured organization wise. Let's see how this can be done.

Onboarding Organizations

1. Login to the WSO2 Identity Server **Console,** using your admin credentials (e.g. admin:admin).
2. In the WSO2 Identity Server **Console,** from the menu click **Organizations.**
3. Then click **+ New Organization**.



Create an Organization

Create a new organization.

Organization Name *

Enter organization name

Description

Enter description

4. Enter **Hospital a** as the organization name and click **Create**.

5. Do the same for **Hospital n**.

Now you have registered Hospital a and Hospital n as organizations in MedVerse.

Create Application and Share with Organizations

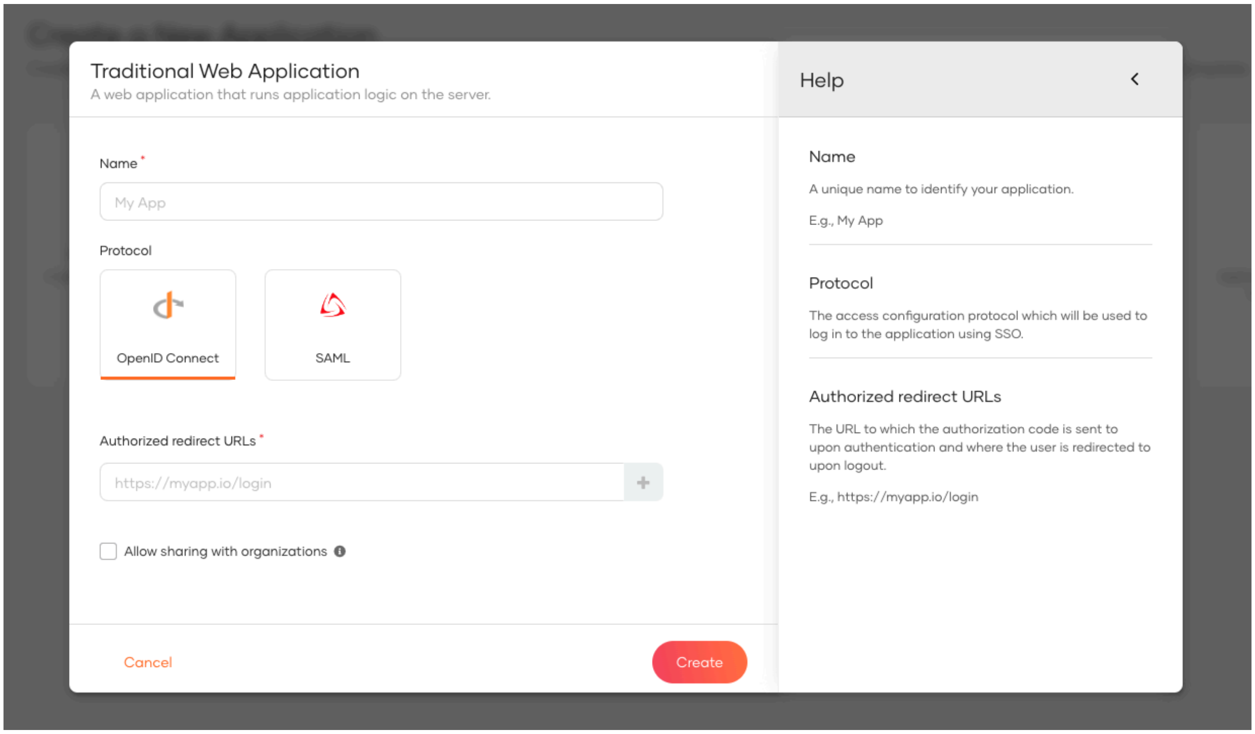
1. In the WSO2 Identity Server **Console,** from the menu click **Applications.**
2. Click **New Application.**
3. From the given set of templates select **Traditional Web Application** template.
4. Fill the fields in the create application wizard.

   Name: *playground2*

   Protocol: *OpenID Connect*

   Authorized redirect URLs:

   http://localhost:8080/playground2/oauth2client



Traditional Web Application

A web application that runs application logic on the server.

Name *

My App

Protocol

OpenID Connect

SAML

Authorized redirect URLs *

https://myapp.io/login

□ Allow sharing with organizations

Help

Name

A unique name to identify your application.

E.g., My App

Protocol

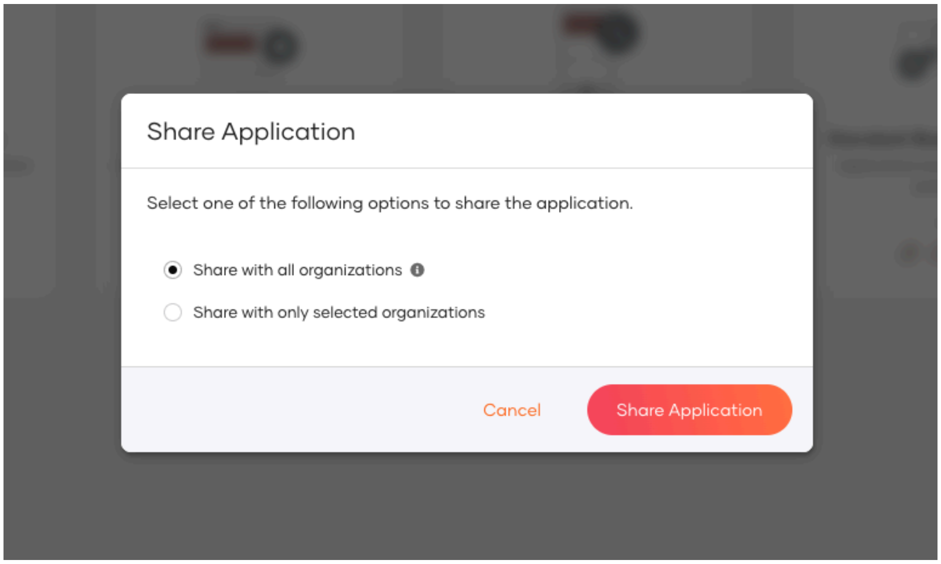
The access configuration protocol which will be used to log in to the application using SSO.

Authorized redirect URLs

The URL to which the authorization code is sent to upon authentication and where the user is redirected to upon logout.

E.g., https://myapp.io/login

5. Click on Allow sharing with organizations and click create.



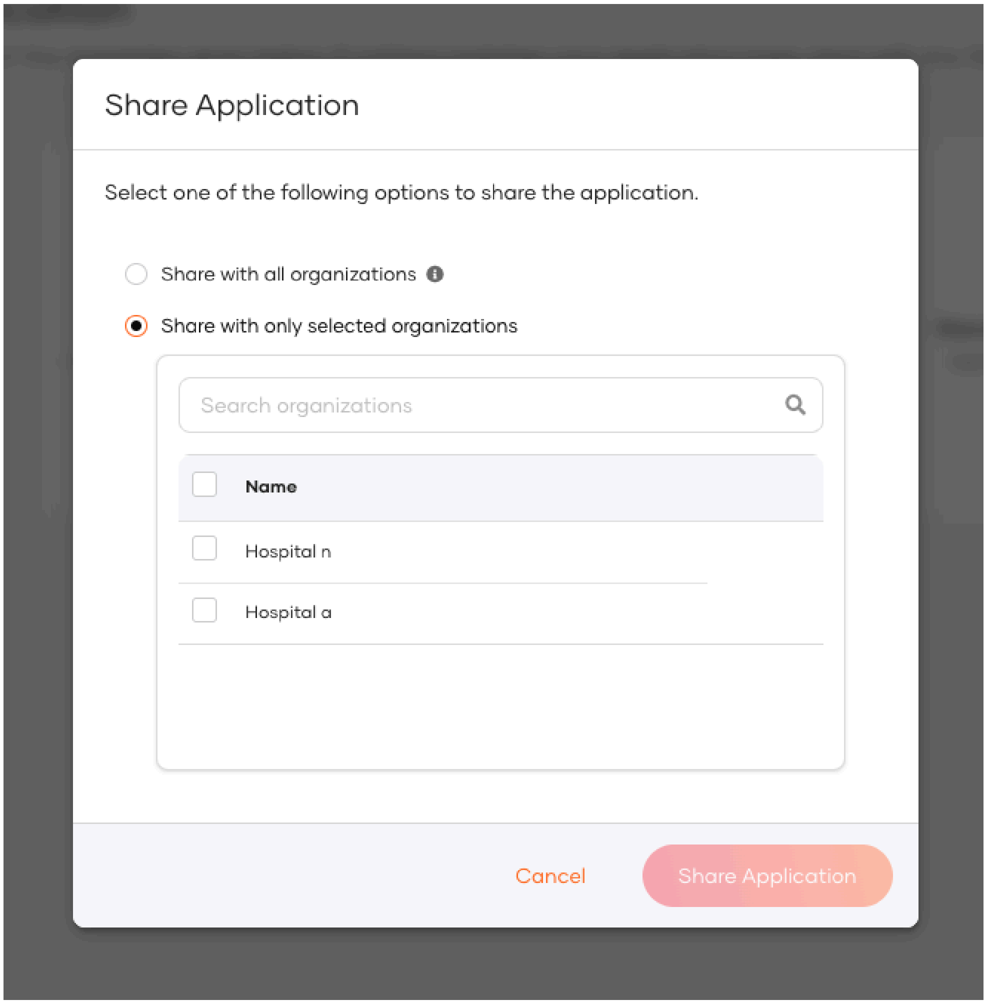
Share Application

Select one of the following options to share the application.

● Share with all organizations

○ Share with only selected organizations

6. Select **Share with only selected organizations**.



Share Application

Select one of the following options to share the application.

○ Share with all organizations

● Share with only selected organizations

□	Name
□	Hospital n
□	Hospital a

7. Select **Hospital a** and **Hospital n** as options and click **Share Application**.
8. Make a note of the **Client ID** of this registered OAuth/OpenID Connect service provider.

Onboarding Organizations Users

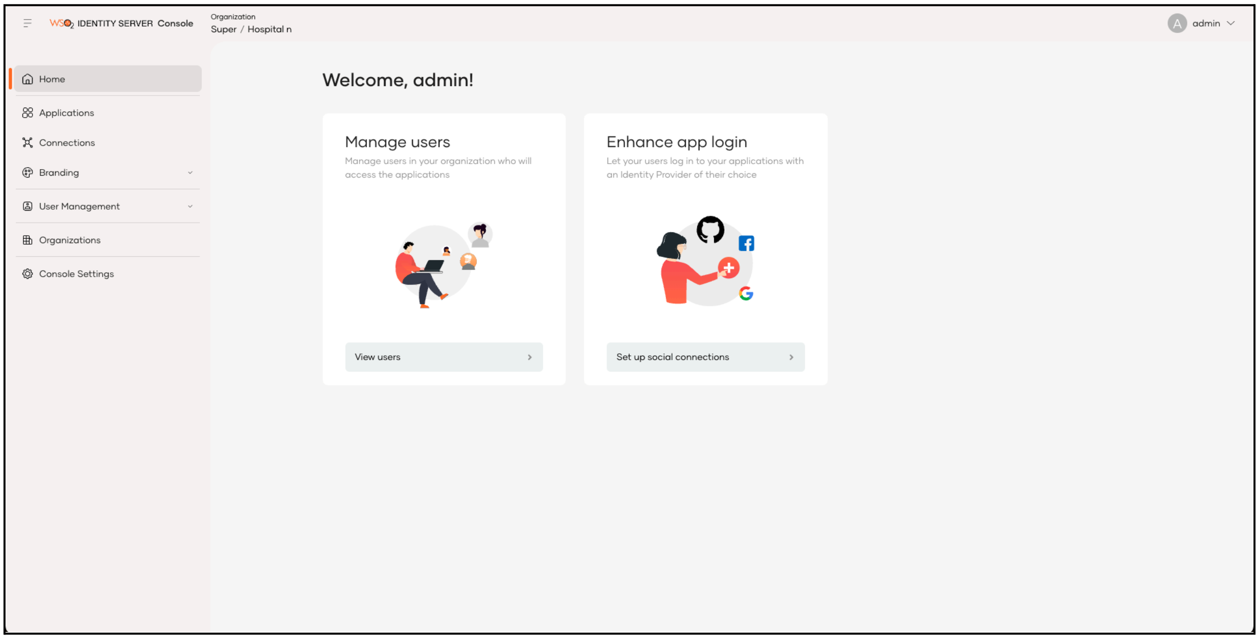
As of now user **admin** has Administrative privileges over both the hospitals. Therefore admin will be creating users in both **Hospital a** and **Hospital n**.

1. Switch Organization

I. In the WSO2 Identity Server **Console,** from the menu click **Organizations.**

II. In the given list of organizations, click on the switch button of **Hospital n**.

III. You will be redirected to the **Console** of Hospital n.



Welcome, admin!

Manage users

Manage users in your organization who will access the applications

Enhance app login

Let your users log in to your applications with an Identity Provider of their choice

2. Create Users

I. Expand the **User Management** menu item from the menu and click **Users.**

II. On the **Users page**, click **Add User** and select **Single User** from the dropdown.

III. To create patient **Tommy**, fill all required fields and click **Finish**.

3. Edit Application

I. Click on the **Applications** from the menu.

II. You will see playground2 listed as an application in the organization **Hospital n**.

III. Click **edit**.

IV. Let's add **Email OTP** as the 2nd step in the authentication.

   A. Click on the plus icon followed by the first screen.

   B. Then click **+ Add Sign In Option**.

   C. Select **Email OTP** as authentication.

V. Click **Update**.

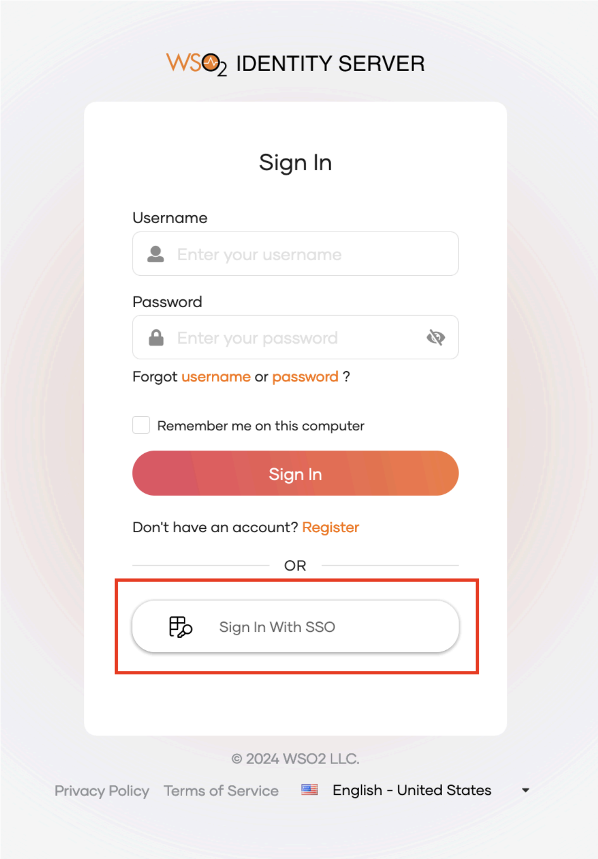
Now follow the same steps from 1-3 for the **Hospital a**.

1. Add a patient name with **Kate**.
2. Leave the Application **Login Flow** as it is.

Try it

Let’s try out the B2B use case using the configured Applications, Organization and Users.

1. Access the playground2 app via http://localhost:8080/playground2/oauth2.jsp
2. Enter the client ID of the service provider registered in IS1 in the **Client ID** field.
3. Click **Authorize**. The browser will be redirected to the login page Application registered in the root organization.
4. Select **Sign in with SSO** option to go to the organization login.



WSO2 IDENTITY SERVER

Sign In

Username

Enter your username

Password

Enter your password

Forgot username or password ?

□ Remember me on this computer

Sign In

Don't have an account? Register

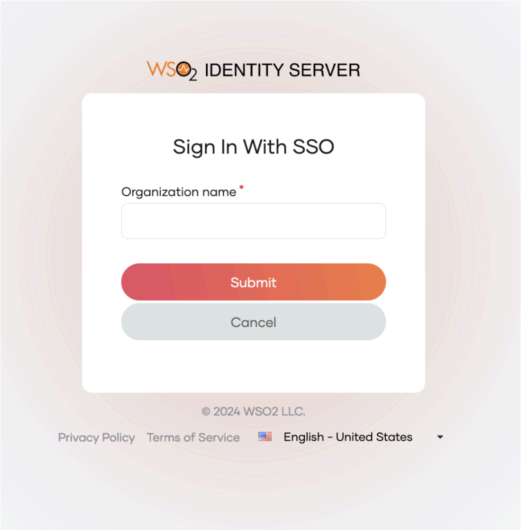
OR

Sign In With SSO

© 2024 WSO2 LLC.

Privacy Policy Terms of Service English - United States

5. Then type the organization name as **Hospital n** and click **Submit**.



6. You will be directed to the organization login screen.
7. Once you enter credentials of **Tommy** you will get redirected to the email OTP page as we have configured **MFA** for **Hospital n** Login Flow.
8. Try the steps from 1-7 with **Hospital a** details and users. You will only get one login step.
9. From that login page select the IDP-IS2 option to authenticate users from the IS2.